Gefahren durch Computer-Viren: Ein Überblick

Einführungs-Whitepaper zu Viren und anderen Formen von „Malware“

Autor: April Goostree, Virus Research Manager

Herausgeber: Samuel Curry, Security Architect, Director or Product Marketing

McAfee.com Corporation, 535 Oakmead Parkway

Sunnyvale, CA 94086

Version: 1.0

Datum: 11.09.2001

Gefahren durch Computer-Viren: Ein Überblick

Was ist ein Computervirus? Welche Infektionswege gibt es? Und angesichts der Tatsache, dass jeden Monat 300 bis 400 neue Viren entdeckt werden: Wie kann man seinen PC dagegen schützen? Diese und andere Fragen werden wir in dem vorliegenden Whitepaper klären.

Denken Sie immer daran: Trotz aller Abwehrmaßnahmen sind Sie niemals 100% immun gegen Computer-Viren – außer Sie benutzen keinen Computer! Die Informationen und Anregungen in diesem Paper sollen Ihnen als Entscheidungshilfe dienen, wenn es um Viren-Schutz für Ihre Rechnersysteme geht, der Ihre speziellen Anforderungen gezielt erfüllt. Wenn Sie Fragen zu einem der hier besprochenen Themen haben, wenden Sie sich bitte an den technischen Support von McAfee.com unter http://www.mcafee.com/support/default.asp

Was ist ein Virus?

Diese unangenehmen und manchmal auch sehr zerstörerischen Programme finden immer wieder ein großes Medien-Echo. Wenn man es aber nüchtern betrachtet, ist ein Computervirus nur eine Datei, die sich auf einer Festplatte einnisten oder an andere Files anhängen kann und sich dann immer wieder selbst vervielfältigt – in der Regel ohne Wissen oder Erlaubnis des Benutzers. Einige Viren hängen sich an Dateien an und werden mit Öffnen dieser Dateien gestartet. Andere laden sich in den Hauptspeicher eines Rechners und infizieren Dateien, die im Computer gerade geöffnet, geändert oder angelegt werden. Manche Computer-Viren machen nichts anderes, als sich lediglich selbst zu kopieren, wohingegen andere riesige Schäden durch Geschäfts-ausfälle, Datenverluste und Produktivitätsminderungen anrichten können.

Es wurden Computerviren für viele Betriebssysteme geschrieben, unter anderem für DOS, Windows, Amiga, Macintosh, Atari und UNIX. Ziel von Antiviren-Software wie ActiveShield und VirusScan Online-Services von McAfee.com ist der Schutz der Anwender gegen diese überall lauernde und ständig wachsende Bedrohung. Derzeit erkennt die Antiviren-Software von McAfee.com über 63.000 Viren, Trojanische Pferde und andere Formen von heimtückischer Software, die auch als „Malware“ bezeichnet wird.

Kategorien von Viren und anderer Malware

Der Begriff „Virus“ ist ein Oberbegriff zur allgemeinen Bezeichnung von Computer-Malware, der sich wiederum in Unterkategorien aufteilen lässt. In diesem Abschnitt vermitteln wir Ihnen genauere Informationen über die unterschiedlichen Arten von Gefahren.

Die Virus-Klasse lässt sich im Wesentlichen in drei Kategorien unterteilen:

1. **Datei-Viren—**Diese hängen sich in der Regel an COM- oder EXE-Dateien an bzw. ersetzen diese. Sie können auch Dateien mit den Erweiterungen SYS, DRV, BIN, OVL und OVY infizieren.

   Die meisten dieser Datei-Viren laden sich in den Hauptspeicher und bleiben dort resident. Viele nicht residente Viren befallen einfach eine oder mehrere Files, sobald eine infizierte Datei geöffnet wird. Der neueste publizierte Datei-Virus ist der W32/Magistr.b**:** http://vil.mcafee.com/dispVirus.asp?virus_k=99199&

2. **Makro-Viren**—Ein Makro ist eine Abfolge von Instruktionen, die Routine-Aufgaben in einem Programm wie Microsoft Word, Excel oder Access vereinfachen. Diese werden ausgeführt, wenn ein Benutzer eine zugehörige Datei öffnet. *Makro-Viren* sind sehr heimtückisch. Sie werden in einer Makro-Programmiersprache geschrieben und an eine Dokumentdatei (wie Word oder Excel) angehängt. Sobald Dokumente oder Formatvorlagen („Templates“), die einen derartigen Virus enthalten, in der Ziel-Applikation geöffnet werden, startet der Virus, richtet seinen Schaden an und kopiert sich in andere Dokumente vom selben Dateityp.

   Die laufende Nutzung des infizierten Programms bewirkt die Verbreitung des Virus. Ein Beispiel für einen weit verbreiteten Makro-Virus ist W97M/Ethan.gen: http://vil.mcafee.com/dispVirus.asp?virus_k=10107&

3. **Boot-Sektor-Virus—**Dieser Virus legt seinen Start-Code im Boot-Sektor ab; das ist ein Bereich, der sich auf der ersten Spur von Disketten und logischen Plattenlaufwerken befindet, die den so genannten Boot-Record enthalten. Dieser Datensatz enthält Informationen über die Eigenschaften und den Inhalt der Disk sowie Informationen, die zum Starten des Computers erforderlich sind. Wenn der Computer die Instruktionen im Boot-Sektor liest und ausführt, wird der Virus in den Hauptspeicher geladen, wo er die Kontrolle über grundlegende Computer-Operationen übernehmen kann. Vom Hauptspeicher kann sich ein Boot-Sektor-Virus auf andere Laufwerke im System verbreiten (Diskette, Netzwerk usw.). Ein gutes Beispiel für einen Boot-Sektor-Virus ist der ByeBye Virus: http://vil.mcafee.com/dispVirus.asp?virus_k=98546&

Zusätzlich zur Klasse der Viren gibt es noch Würmer, Trojanische Pferde und Hoax-Viren (Warnungen vor Viren, die es nicht gibt):

1. **Würmer**—Dabei handelt es ich um Parasiten-Programme, die sich vervielfältigen, aber im Gegensatz zu Viren keine anderen Programmdateien befallen. Würmer erzeugen ihre Kopien entweder nur auf einem Rechner oder verschicken diese über ein Netzwerk oder E-Mail-Programm auch an andere Computer. Sie können sich auch über IRC (Internet Relay Chat) verbreiten. Wie Viren sind auch Würmer in der Lage, eine schleichende Infektion ohne das Wissen des Opfers zu verursachen, oder sofortiges Chaos auf einem System anzurichten. In der Vielzahl der Fälle werden Würmer erst bemerkt, wenn ihre unkontrollierte Vervielfältigung einen hohen Verbrauch von Systemressourcen zur Folge hat oder durch große Mengen von ausgehender E-Mails sichtbar wird, die nicht vom Opfer stammen. VBS/Loveletter ist ein berüchtigtes Beispiel für eine solchen Wurm: http://vil.mcafee.com/dispVirus.asp?virus_k=98617&

2. **Trojanische Pferde**—Dies ist ein heimtückischer oder schädlicher Code, der sich in scheinbar harmlosen Programmen oder Dateien befindet. Oft wird der gefährliche Code in Computer-Spielen oder Grafikdateien versteckt, die so zu „Trojanern“ werden. W32/Pretty.

Worm ist ein Beispiel für einen Trojaner, der aufgrund seiner Art sich zu verbreiten auch als Wurm bezeichnet wird:
http://vil.mcafee.com/dispVirus.asp?virus_k=10175&

3. **Hoax**—Ein Viren-Hoax ist ein Fehlalarm. Den dabei angegebenen Namen des Virus gibt es unter Umständen in Wirklichkeit, aber die Nachricht, die mit der Warnung mitgeschickt wird, ist entweder teilweise oder vollkommen aus der Luft gegriffen. In der Regel kommt diese Warnung in einer E-Mail-Nachricht an, die über große Verteilerlisten verschickt wird. In der Mail wird der Empfänger aufgefordert, die Nachricht an möglichst viele Internet-Benutzer weiterzuschicken. Dabei wird ein Gefühl der Dringlichkeit und der drohenden Gefahr vermittelt, wenn die Warnung missachtet wird. Zu ihrer Verbreitung setzen Hoax-Viren auf die Angst der Opfer.
Ein Beispiel für einen Hoax ist der "Internet Flower For You":
http://vil.mcafee.com/dispVirus.asp?virus_k=98604&
Wenn Sie glauben, einen Viren-Hoax erhalten zu haben, nehmen Sie sich einfach die Zeit und prüfen dies auf der Viren-Hoax-Seite von McAfee.com nach: http://vil.mcafee.com/hoax.asp. Die Namen von Hoax-Viren sind unter Umständen ganz anders als Sie vermuten. Wenn Sie nicht sicher sind, schicken Sie bitte eine E-Mail an virus_support@mcafee.com, um die betreffende Nachricht von uns prüfen zu lassen. Da Viren-Falschmeldungen Angst verbreiten, ist es wichtig, dass man sie erkennt und andere über die Täuschung informiert. Leiten Sie Hoax-Viren deshalb nicht weiter.

Wie verbreiten sich Viren und andere Computer-Malware? Gibt es spezielle Vorbeuge-Maßnahmen, die für die einzelnen Verbreitungsmethoden ergriffen werden sollten?

In den Anfangstagen der Viren war der häufigste Verbreitungsweg über Disketten. Vor der Internet-Ära und dem explosionsartigen Wachstum der E-Mail-Nutzung bestand die einfachste Möglichkeit zur Weitergabe von Dateien oder Programme darin, dass man sie auf Diskette kopierte und persönlich übergab. Heute ist der Infektionsweg über Diskette immer noch ein Problem. Hier ein Beispiel: Ein Lehrer gibt Disketten aus, auf denen sich Hausaufgaben befinden.

Diese werden dann in verschiedene PCs eingelegt, die unter Umständen vernetzt sind bzw. die von anderen Mitgliedern eines Haushalts genutzt werden. Damit steigt das Risiko, dass die Diskette infiziert wird. Stellen Sie sich jetzt vor, die Diskette wird tatsächlich infiziert und mit in die Schule genommen. Das Netzwerk der Schule ist jetzt bedroht und jeder Einzelne, der auf das befallene Netzwerk zugreift, setzt sich ebenfalls dieser Gefahr aus. Das ist eines von vielen Beispiele für die Verbreitung von Computerviren per Diskette.

Deshalb besteht die beste Vorbeuge-Möglichkeit gegen diesen Infektionsweg darin, grundsätzlich alle Diskette vor jeder Verwendung auf Viren zu prüfen. Die Prüfung sollte auf einem isolierten System ohne Netzwerkanschluss durchgeführt werden, so dass keine weiteren Infektionen auftreten können, wenn sich die Entfernung eines Virus als unmöglich erweist. Falls Sie einen PC zu Hause nutzen und Disketten zwischen Büro und anderen Systemen übertragen (Schul-Netzwerk, PC von Freunden usw.), ist es ratsam, Ihre Disketten vor dem Öffnen der darauf befindlichen Dateien zu prüfen. Disketten können u.a. Datei-Viren, Trojanische Pferde und Dokumente mit Makro-Viren transportieren. Sie können auch Boot-Sektor-Viren enthalten, die beim Booten von der betreffenden Diskette starten. Deshalb sollten Sie darauf achten, dass das Diskettenlaufwerk Ihres Rechners beim Systemstart immer leer ist.

Der wesentlich „populäre" Weg zur Verbreitung von Viren ist natürlich per E-Mail – die schnellste und effizienteste Möglichkeit, die „schlechte Nachricht" zu verbreiten. Viele Menschen auf der ganzen Welt nutzen das gleiche E-Mail-Programm, weshalb sie leicht zu Opfern eines Viren-Programmierers werden können. In der Regel werden Viren, die per E-Mail verschickt werden, als „Würmer" eingestuft, weil sie Kopien ihres hinterhältigen Codes machen und sich anschließend verbreiten, indem sie diese Kopien an alle Benutzer im E-Mail-Adressbuch des Opfers schicken. Aber praktisch jede andere Art von Virus kann sich auch dieser Verbreitungsmethode bedienen.

Schutz gegen Viren, die per E-Mail verschickt werden, erfordert einige grundlegende Schritte:

1. Installation, Update und regelmäßige Verwendung von Antiviren-Software, die Rund-um-die-Uhr-Schutz bietet und die gezielte Überprüfung einzelner Laufwerke, Ordner oder Platten erlaubt. McAfee.com Clinic besteht aus ActiveShield und VirusScan Online: ActiveShield bietet ständigen Schutz und überwacht Ihre E-Mail-Attachments sowie sämtliche Dateien und Programme, die Sie öffnen. VirusScan Online wird genutzt, wenn Sie eine ganz spezielle Datei oder ein bestimmtes Laufwerk auf Viren hin überprüfen wollen. Das Programm ist auch sehr gut zur Überprüfung eines ganzen PC im Rahmen eines wöchentlichen Wartungsprogramms geeignet.

   Um den maximalen Nutzen zu erzielen, sollte die Antiviren-Software, für die Sie sich entscheiden, benutzerfreundlich und einfach zu aktualisieren sein.

2. Achten Sie auf die Arten von E-Mails, die Sie bekommen, und darauf, von wem Sie sie erhalten sowie welchen Betreff sie enthalten. Entsprechend dem alten Sprichwort „Vorsicht ist die Mutter der Weisheit“ hilft hier gesunder Menschenverstand sehr viel weiter. Wenn Sie beispielsweise regelmäßig von einem Freund E-Mails mit Witzen, Bildern oder einfachen Mitteilungen erhalten, und plötzlich eine Nachricht von ihm bekommen, die wie ein offizielles Dokument aussieht (wie bei der Betreffzeile des kürzlichen W32/Apost@mm Wurms http://vil.mcafee.com/dispVirus.asp?virus_k=99198&**),** dann sollten bei Ihnen die Alarmglocken läuten. Im Mai 2000 erhielten Millionen von Menschen E-Mails, die scheinbar einen „Loveletter“ enthielten. Die meisten dieser E-Mails schienen von Kollegen, Vorgesetzten und Menschen zu kommen, die wohl kaum einen Liebesbrief verschicken würden. Die Warnzeichen waren also alle vorhanden, trotzdem konnte sich „Loveletter“ innerhalb kürzester Zeit verbreiten. Aber hinterher ist man immer klüger.

Fast jeder weiß, dass E-Mail-Viren in Anhängen auftauchen. Nicht bekannt ist jedoch, dass sie auch in einer E-Mail-Nachricht ohne Anhang *versteckt* sein können. Dieser Virentyp wird Script genannt. Scripts benötigen den Windows Scripting Host (wenn Sie mit Windows arbeiten), um ablaufen zu können. Sie werden ohne Intervention des E-Mail-Empfängers ausgeführt – das bedeutet, dass Ihr Rechner infiziert werden kann, ohne dass Sie etwas davon merken! Und noch schlimmer: Sie müssen die infizierten E-Mails nicht einmal ganz öffnen, damit das Script ausgeführt wird. Beispielsweise ist der Bubbleboy Virus ein Visual Basic-Script-Wurm, der schon gestartet wird, wenn Sie die infizierte E-Mail im so genannten Vorschaubereich von Outlook ansehen. Das führt uns zu zwei weiteren Vorsichtsmaßregeln:

1. Deaktivieren Sie den Vorschaubereich Ihres E-Mail-Programms. Wenn Sie den Vorschaubereich eingeblendet haben, arbeiten Sie beim Lesen von E-Mail mit einem geteilten Bildschirm. Der obere Teil zeigt die Liste der eingegangenen Mails, der untere Bildschirmteil zeigt den Inhalt der Nachricht, die oben gerade markiert ist. E-Mails, die im Vorschaubereich angezeigt werden, werden nicht ganz geöffnet, aber einige Script-Viren können über dieses Fenster ohne Ihr Wissen gestartet werden. Deshalb ist es ratsam, die Vorschau abzuschalten. Im Hilfe-Menü eines Windows-basierten Programms finden Sie in aller Regel Hinweise dazu, wie Sie dabei vorgehen müssen.
2. Bei einigen Versionen von Windows ist der Windows Script Host automatisch installiert und aktiviert. Wenn Sie kein Entwickler sind, der diese Funktionalität benötigt, dann ist es ratsam, den Windows Scripting Host zu deaktivieren. Dadurch hindern Sie viele Arten von Scripting-Viren daran, automatisch zu starten.

Der Schlüssel zur „erfolgreichen" Verbreitung eines E-Mail-Virus ist, dass möglichst viele Adressaten den infizierten Anhang öffnen und an andere Opfer weiterschicken. Aus diesem Grund werden Würmer zur Zeit so häufig verwendet. Je mehr Menschen Würmer öffnen, desto mehr Gelegenheit haben diese, ihren heimtückischen Code an eine große Anzahl anderer Computer-Benutzer zu verschicken, die ihn dann öffnen – es entsteht so ein richtiger Schneeball-Effekt.

Aber wie stellen die Virenprogrammierer sicher, dass eine große Anzahl von Menschen einen infizierten E-Mail-Anhang öffnen? Sie arbeiten mit Täuschungsmanövern, die auf menschliche Schwächen setzen. Das bekannteste Beispiel ist der Loveletter-Virus. Nur die wenigsten Menschen konnten der Versuchung widerstehen, einen Blick in einen potenziellen Liebesbrief zu werfen ... insbesondere, da er direkt an sie adressiert war (siehe 2. „Der Schutz gegen Viren, die per E-Mail verschickt werden" oben)! Hier gilt: „Wenn der Inhalt zu gut klingt, um wahr zu sein, dann ist er das wahrscheinlich auch." Erliegen Sie nicht der Versuchung. Der Loveletter-Virus verursachte einen Schaden von geschätzten 8 bis 11 Milliarden Dollar weltweit. Ein weiteres Beispiel ist der **W32/Naked@mm** Wurm, der angeblich ein Video einer nackten Frau als Anhang enthielt, aber in Wirklichkeit verschiedene Dateien und Systemordner löschte und sich gleichzeitig eigenständig an alle Anwender im Adressbuch des Opfers verschickte.

Viren und andere Malware können neben Disketten oder E-Mails auch noch andere Infektionswege nutzen:

1. **Web-Seiten**—Wenn Sie auch auf „anrüchigen" Seiten surfen, gehen Sie das Risiko ein, auf einer Site zu landen, die unsichere Scripts enthält. Das kann zu einer Infektion und oft zu einer noch ernsteren Sicherheitsverletzung führen. Backdoor-Trojaner werden am häufigsten über zweifelhafte Web-Sites übertragen. Sobald sie sich auf Ihrem System befinden, können sie in einer Vielzahl der Fälle private und/oder persönliche Informationen zurück an den Betreiber der Site schicken.

2. **DSL- und Kabelmodem-Verbindungen**—PC-Benutzer, die mit ständig aktiven Internet-Verbindungen arbeiten, haben im Prinzip eine Tür zu ihrem Rechner geöffnet. Diese führt zum gesamten Internet, und jeder, der über ausreichendes Hacker-Wissen verfügt, kann diese Tür finden und eintreten. Auch hier sprechen wir von Sicherheitsverletzungen, die immer schwerwiegend sind – vollkommen unabhängig von den Informationen, die abgerufen werden. Persönliche Informationen sollten nie in die Hände von Unbefugten fallen.

Der Schlüssel zur Vermeidung dieser Infektionsmethoden ist die Errichtung und Verwendung einer persönlichen Firewall. Diese fungiert als Wächter an der Tür, die von Ihrem PC zum Internet führt. Die Firewall beobachtet alles, was herein kommt oder hinaus geht. Wenn der Verdacht auf eine Unregelmäßigkeit besteht, werden Sie darauf aufmerksam gemacht. Wenn Sie eine Web-Seite ansteuern, die versucht, heimtückischen Code in Ihren Rechner zu laden, verhindert eine Firewall diesen Download und setzt Sie über diesen Vorfall in Kenntnis. Wenn ein Hacker eine „offene Tür" an Ihrem PC findet und einzudringen versucht, verhindert dies die Firewall ebenfalls und macht Sie auch in diesem Fall auf das Ereignis aufmerksam. Persönliche Firewalls sind eine wichtige zusätzliche Schutzschicht, die jeder installieren sollte, der mit einer ständigen aktiven Verbindung zum Internet arbeitet und/oder viel auf fragwürdigen Web-Sites surft.

Schließlich sind noch Netzwerke und gemeinsam genutzte Laufwerke/Dateien/Ordner als Verbreitungswege für Viren zu erwähnen. Ein Netzwerk können Sie sich wie ein Gebäude mit vielen Räumen vorstellen. Jeder Raum hat eine Tür mit Schloss. Wenn Sie mit anderen Menschen vernetzt sind und ihnen die Inhalte Ihres Raums zugänglich machen (und umgekehrt), dann haben Sie die Türen zu diesen Räumen nicht zugesperrt. Jeder könnte hereinspazieren – auch Unbefugte – und damit eine Sicherheitsverletzung verursachen. Es könnten nicht nur Informationen gestohlen, sondern auch Viren und andere heimtückische Programme in Umlauf gebracht werden. Solche Umgebungen lassen sich durch die Implementierung von Passwörtern schützen. Diese verhindern unbefugten Zugang zu Laufwerken und ihren Inhalten (Räume sind nur mit dem passenden Schlüssel betretbar), und können auf jeder Ebene implementiert werden (d.h. für ein Laufwerk, für einen Ordner oder auch gezielt für nur eine bestimmte Datei). Je restriktiver der Passwort-Schutz gehandhabt wird, desto sicherer ist Ihr gesamtes Netzwerk und dessen Inhalte. Ein letztes Beispiel: Würmer können sich über Netzwerke und E-Mail-Programme verbreiten. Wenn Ihre gemeinsam genutzten Netzwerk-Laufwerke passwort-geschützt sind, wird ein Wurm, der auf einem PC in diesem Netzwerk eingeschleust wurde, durch die Passwort-Abfrage an der Verbreitung gehindert.

Abschließend lässt sich sagen, dass wir nur ganz oberflächlich auf das Problem von Viren und anderer Malware eingehen konnten. Die Art, wie Viren angreifen, was sie anrichten und wie sie sich tarnen, entwickelt sich ständig weiter. Die beste Verteidigungsstrategie basiert auf drei Säulen: Nutzen Sie die richtigen Tools – in diesem Fall eine gute und aktuelle Antiviren- und Firewall-Software. Halten Sie sich über das Geschehen in der Welt der Online-Gefahren auf dem Laufenden. Und überprüfen Sie immer wieder die Tools und Maßnahmen, die Sie zu Hause und am Arbeitsplatz implementiert haben, um sicherzustellen, dass Ihre Informations-Ressourcen geschützt sind.